

# AUTOMORPHISMS OF ORDER $2p$ IN BINARY SELF-DUAL EXTREMAL CODES OF LENGTH A MULTIPLE OF 24

Martino Borello

Università degli Studi di Milano Bicocca  
Milano, Italy  
`m.borello1@campus.unimib.it`

Wolfgang Willems

Otto-von-Guericke Universität,  
Magdeburg, Germany,  
`willems@ovgu.de`

Version of September 22, 2012, printed September 27, 2012

## Abstract

Let  $C$  be a binary self-dual code with an automorphism  $g$  of order  $2p$ , where  $p$  is an odd prime, such that  $g^p$  is a fixed point free involution. If  $C$  is extremal of length a multiple of 24 all the involutions are fixed point free, except the Golay Code and eventually putative codes of length 120. Connecting module theoretical properties of a self-dual code  $C$  with coding theoretical ones of the subcode  $C(g^p)$  which consists of the set of fixed points of  $g^p$ , we prove that  $C$  is a projective  $\mathbb{F}_2\langle g \rangle$ -module if and only if a natural projection of  $C(g^p)$  is a self-dual code. We then discuss easy to handle criteria to decide if  $C$  is projective or not. As an application we consider in the last part extremal self-dual codes of length 120, proving that their automorphism group does not contain elements of order 38 and 58.

KEY WORDS: self-dual codes, automorphism group

## 1 Introduction

Binary self-dual extremal codes of length a multiple of 24 are binary self-dual codes with parameters  $[24m, 12m, 4m + 4]$ . They are interesting for various algebraic and geometric reasons; for example, they are doubly even [14] and all codewords of a fixed given nontrivial weight support a 5-design [1]. Very few is

known about this family of codes: for  $m = 1$  we have the Golay Code  $\mathcal{G}_{24}$  and for  $m = 2$  there is the extended quadratic residue code  $XQR_{48}$ , but no other examples are known so far.

A classical way of approaching the study of such codes is through the investigation of their automorphism group. In this paper we focus our attention to automorphisms of order  $2p$ , where  $p$  is an odd prime. There are elements of this type in the automorphism group of  $\mathcal{G}_{24}$  and  $XQR_{48}$ , while it was recently proved [2] that for  $m = 3$  no automorphisms of order  $2p$  occur. The problem is totally open for  $m > 3$ . It is known [5] that for  $m \notin \{1, 5\}$  the involutions are fixed point free. So we will restrict our study to those automorphisms  $g$  of order  $2p$  whose  $p$ -power acts fixed point freely.

In the first part of the paper we connect module theoretical properties of a self-dual code  $C$  with coding theoretical ones of the subcode  $C(g^p)$  which consists of the fixed points of  $g^p$ . More precisely, we prove in Theorem 1 that  $C$  is a projective  $\mathbb{F}_2\langle g \rangle$ -module if and only if a natural projection of  $C(g^p)$  is a self-dual code. In the second part, i.e. section 4, we apply these results to the case  $m = 5$ . In particular we prove that there are no automorphisms of order  $2 \cdot 19$  and  $2 \cdot 29$ . All computations of the last part are carried out with MAGMA [6].

## 2 Preliminaries

From now on a code always means a binary linear code and  $K$  always denotes the field  $\mathbb{F}_2$  with two elements.

Let  $C$  be a code and let  $g \in \text{Aut}(C)$ . We denote by

$$C(g) = \{c \in C \mid c^g = c\}$$

the subcode of  $C$  consisting of all codewords which are fixed by  $g$ . It is easy to see that a codeword  $c = (c_1, \dots, c_n)$  is fixed by  $g$  if and only if  $c_i = c_{i^g}$  for every  $i \in \{1, \dots, n\}$ , i.e., if and only if  $c$  is constant on the orbits of  $g$ .

**Definition 1.** For an odd prime  $p$  let  $s(p)$  denote the smallest  $s \in \mathbb{N}$  such that  $p \mid 2^s - 1$ . Note that  $s(p)$  is the multiplicative order of 2 in  $\mathbb{F}_p^*$ .

The next lemma is a well-known fact in modular representation theory. For the basics in this theory (and only those are needed in this article) the reader is referred to chapter VII of [12].

**Lemma 1.** Let  $\nu = \frac{p-1}{s(p)}$ , where  $p$  is an odd prime, and let  $G = \langle g \rangle$ . If  $g$  is of order  $2p$  then we have.

- a) There are  $1 + \nu$  irreducible  $KG$ -modules  $V_0, V_1, \dots, V_\nu$ , where  $V_0 = K$  (the trivial module) and  $\dim V_i = s(p)$  for  $i \in \{1, \dots, \nu\}$ .
- b) For  $i = 0, \dots, \nu$  the projective indecomposable cover  $W_i$  of  $V_i$ , called a PIM, is a nonsplit extension  $W_i = \begin{smallmatrix} V_i \\ V_i \end{smallmatrix}$  of  $V_i$  by  $V_i$ . Furthermore,

$$KG = W_0 \oplus W_1 \oplus \dots \oplus W_\nu.$$

In order to understand codes with automorphisms of order  $2p$  we need the following result which improves Proposition 3.1 of [13].

**Proposition 1.** *Let  $G = \langle g \rangle$  be a cyclic group of odd prime order  $p$ .*

- a) *If  $s(p)$  is even, then all irreducible  $KG$ -modules are self-dual.*
- b) *If  $s(p)$  is odd, then the trivial module is the only self-dual irreducible  $KG$ -module.*

*Proof.* a) Let  $s(p) = 2t$  and let  $E = \mathbb{F}_{2^{2t}}$  be the extension field of  $K = \mathbb{F}_2$  of degree  $2t$ . Furthermore, let  $W$  be an irreducible nontrivial  $KG$ -module. In particular,  $W$  has dimension  $2t$ . By Theorem 1.18 and Lemma 1.15 in Chap. VII of [12], we have

$$W \otimes_K E = \bigoplus_{\alpha \in \text{Gal}(E/K)} V^\alpha \quad (1)$$

where  $V$  is an irreducible  $KG$ -module and  $V^\alpha$  is the  $\alpha$ -conjugate module of  $V$ . Since  $p \mid (2^t + 1)(2^t - 1)$  we get  $p \mid 2^t + 1$ . Clearly,  $\text{Gal}(E/K)$  consists of all automorphisms of the form  $x \mapsto x^k$  where  $0 \leq k \leq 2t - 1$ .

If  $V = \langle v \rangle$  then  $vg = \epsilon v$  where  $\epsilon$  is a nontrivial  $p$ -th root of unity in  $E$ . Since  $p \mid 2^t + 1$  we obtain  $\epsilon^{2^t+1} = 1$ , hence  $\epsilon^{2^t} = \epsilon^{-1}$ . Thus there is an  $\alpha \in \text{Gal}(E/K)$  such that

$$V^* \cong V^\alpha$$

and equation (1) implies  $W \cong W^*$ .

b) Now let  $s(p) = t$  be odd. As above the irreducible module  $W$  is self-dual if and only if  $V \cong V^\alpha$  for some  $\alpha \in \text{Gal}(\mathbb{F}_{2^t}/K)$ , or equivalently if and only if  $\epsilon^\alpha = \epsilon^{-1}$ . Suppose that such an  $\alpha$  exists. Then we may write  $\epsilon^\alpha = \epsilon^{2^k}$  where  $0 \leq k \leq t - 1$ . Hence  $\epsilon^{2^k} = \epsilon^{-1}$  for some  $0 \leq k \leq t - 1$  and therefore  $2^k \equiv -1 \pmod{p}$ . Now  $2^{2k} \equiv 1 \pmod{p}$  forces  $t \mid 2k$ . Since  $t$  is odd we get  $t \mid k \leq t - 1$ , a contradiction.  $\square$

**Remark 1.** According to Lemma 3.5 in [13] we have  $s(p)$  even if  $p \equiv \pm 3 \pmod{8}$  and  $s(p)$  odd if  $p \equiv -1 \pmod{8}$ .

**Remark 2.** Since  $KG \cong KG^*$ , Lemma 1 and Proposition 1 imply the following.

- a) If  $s(p)$  is even, then

$$KG = W_0 \oplus W_1 \oplus \dots \oplus W_\nu$$

with  $W_i \cong W_i^*$  for all  $i \in \{0, \dots, \nu\}$ .

- b) If  $s(p)$  is odd, then  $\nu$  is even (put  $\nu = 2t$ ) and

$$KG = W_0 \oplus W_1 \oplus \dots \oplus W_{2t}$$

with  $W_0 \cong W_0^*$  and  $W_i \cong W_{2i}^*$  for all  $i \in \{1, \dots, t\}$ .

### 3 Automorphisms of order $2p$ in self-dual codes

Throughout this section let  $C$  be a self-dual code of length  $n$ . In particular  $n$  is even. Suppose that  $g \in \text{Aut}(C)$  is of order  $2p$ , where  $p$  is an odd prime. Furthermore suppose that the involution  $h = g^p$  acts fix point freely on the  $n$  coordinates. Without loss of generality, we may assume that  $h = g^p = (1, 2)(3, 4) \dots (n-1, n)$ .

We consider the maps  $\pi = \pi_2 : C(h) \rightarrow K^{\frac{n}{2}}$ , where

$$(c_1, c_1, c_2, c_2, \dots, c_{\frac{n}{2}}, c_{\frac{n}{2}}) \xrightarrow{\pi} (c_1, c_2, \dots, c_{\frac{n}{2}}),$$

and  $\phi : C \rightarrow K^{\frac{n}{2}}$ , where

$$(c_1, c_2, \dots, c_{n-1}, c_n) \xrightarrow{\phi} (c_1 + c_2, \dots, c_{n-1} + c_n).$$

According to Theorem 1 of [3] we have

$$\phi(C) \subseteq \pi(C(h)) = \phi(C)^\perp.$$

In particular,

$$\phi(C) = \pi(C(h)) = \phi(C)^\perp \quad (\text{i.e. } \pi(C(h)) \text{ is self-dual})$$

if and only if

$$\dim \pi(C(h)) = \dim C(h) = \frac{n}{4}.$$

**Theorem 1.** *The code  $C$  is a projective  $K\langle g \rangle$ -module if and only if  $\pi(C(h))$  is a self-dual code.*

*Proof.* First note that for an arbitrary finite group  $G$  a  $KG$ -module is projective if and only if its restriction to a Sylow 2-subgroup is projective ([12], Chap. VII, Theorem 7.14). Thus we have to consider the restriction  $C|_{\langle h \rangle}$ , i.e.,  $C$  with the action of  $\langle h \rangle$ . As a  $K\langle h \rangle$ -module we may write

$$C \cong \underbrace{R \oplus \dots \oplus R}_{a \text{ times}} \oplus \underbrace{K \oplus \dots \oplus K}_{\frac{n}{2} - 2a \text{ times}},$$

where  $R$  is the regular  $K\langle h \rangle$ -module and  $K$  is the trivial one. If  $\text{soc}(C)$  denotes the socle of  $C$ , i.e. the largest completely reducible  $K\langle h \rangle$ -submodule of  $C$ , then

$$C(h) = \text{soc}(C) = \underbrace{K \oplus \dots \oplus K}_{a \text{ times}} \oplus \underbrace{K \oplus \dots \oplus K}_{\frac{n}{2} - 2a \text{ times}} \cong K^{\frac{n}{2} - a}.$$

Thus  $C$  is projective if and only if  $\frac{n}{2} - 2a = 0$ , hence if and only if  $a = \frac{n}{4}$ . This happens if and only if  $\dim C(h) = \frac{n}{4}$ . This is equivalent to the fact that  $\pi(C(h))$  is self-dual.  $\square$

**Remark 3.** If  $n \equiv 2 \pmod{4}$ , then  $\pi(C(h)) \subseteq K^{\frac{n}{2}}$  can not be self-dual, since  $\frac{n}{2}$  is odd.

**Remark 4.** In  $\mathcal{G}_{24}$  and  $XQR_{48}$  the subcodes fixed by fixed point free acting involutions have self-dual projections. Thus we wonder if this holds true for all extremal self-dual codes of length a multiple of 24.

Next we deduce some properties of  $C$  related to the action of the automorphism  $g$  of order  $2p$ . This may help to decide whether  $\pi(C(h))$  is self-dual or not. For completeness we treat both cases  $n \equiv 2 \pmod{4}$  and  $n \equiv 0 \pmod{4}$ .

Since  $h$  acts fixed point freely,  $g$  has  $x$   $2p$ -cycles and  $w$  2-cycles, with

$$n = 2px + 2w. \quad (2)$$

Thus, as a  $K\langle g \rangle$ -module, we have the decomposition

$$K^n = \underbrace{K\langle g \rangle \oplus \dots \oplus K\langle g \rangle}_{x \text{ times}} \oplus \underbrace{K\langle h \rangle \oplus \dots \oplus K\langle h \rangle}_{w \text{ times}}.$$

Using Lemma 1 and  $V_0 \cong K$ , we get

$$K^n = \underbrace{\begin{matrix} V_0 \\ V_0 \end{matrix} \oplus \dots \oplus \begin{matrix} V_0 \\ V_0 \end{matrix}}_{x+w \text{ times}} \oplus \dots \oplus \underbrace{\begin{matrix} V_\nu \\ V_\nu \end{matrix} \oplus \dots \oplus \begin{matrix} V_\nu \\ V_\nu \end{matrix}}_{x \text{ times}}.$$

The action of  $\langle g \rangle$  on  $K^n$  and the self-duality of  $C$  restrict the possibilities for  $C$  as a subspace of  $K^n$ .

More precisely, we have

**Proposition 2.** *As a  $K\langle g \rangle$ -module the code  $C$  has the following structure.*

$$\begin{aligned} C = & \underbrace{\begin{matrix} V_0 \\ V_0 \end{matrix} \oplus \dots \oplus \begin{matrix} V_0 \\ V_0 \end{matrix}}_{y_0 \text{ times}} \oplus \underbrace{V_0 \oplus \dots \oplus V_0}_{z_0 \text{ times}} \oplus \dots \\ & \dots \oplus \underbrace{\begin{matrix} V_\nu \\ V_\nu \end{matrix} \oplus \dots \oplus \begin{matrix} V_\nu \\ V_\nu \end{matrix}}_{y_\nu \text{ times}} \oplus \underbrace{V_\nu \oplus \dots \oplus V_\nu}_{z_\nu}, \end{aligned}$$

where

- 1)  $2y_0 + z_0 = x + w$ ,
- 2a)  $2y_i + z_i = x$  for all  $i \in \{1, \dots, \nu\}$ , if  $s(p)$  is even,
- 2b)  $z_i = z_{2i}$  and  $y_i + y_{2i} + z_i = x$  for all  $i \in \{1, \dots, t\}$ , if  $s(p)$  is odd.

*Proof.* Since  $C = C^\perp$  we see by a proof similar to that of Proposition 2.3 in [15] that  $K^n/C \cong C^*$ . The conditions on the multiplicities are an easy consequence of this fact. Let us prove, for example, part 2b): if

$$C = \dots \oplus \underbrace{\begin{matrix} V_i \\ V_i \end{matrix} \oplus \dots \oplus \begin{matrix} V_i \\ V_i \end{matrix}}_{y_i \text{ times}} \oplus \underbrace{V_i \oplus \dots \oplus V_i}_{z_i \text{ times}} \oplus \dots$$

$$\dots \oplus \underbrace{\begin{matrix} V_{2i} \\ V_{2i} \end{matrix} \oplus \dots \oplus \begin{matrix} V_{2i} \\ V_{2i} \end{matrix}}_{y_{2i} \text{ times}} \oplus \underbrace{V_{2i} \oplus \dots \oplus V_{2i}}_{z_{2i}} \oplus \dots,$$

then

$$K^n/C = \dots \oplus \underbrace{\begin{matrix} V_i \\ V_i \end{matrix} \oplus \dots \oplus \begin{matrix} V_i \\ V_i \end{matrix}}_{x-z_i-y_i \text{ times}} \oplus \underbrace{V_i \oplus \dots \oplus V_i}_{z_i \text{ times}} \oplus \dots$$

$$\dots \oplus \underbrace{\begin{matrix} V_{2i} \\ V_{2i} \end{matrix} \oplus \dots \oplus \begin{matrix} V_{2i} \\ V_{2i} \end{matrix}}_{x-z_{2i}-y_{2i} \text{ times}} \oplus \underbrace{V_{2i} \oplus \dots \oplus V_{2i}}_{z_{2i}} \oplus \dots$$

and since  $V_i \cong V_{2i}^*$ ,

$$C^* = \dots \oplus \underbrace{\begin{matrix} V_{2i} \\ V_{2i} \end{matrix} \oplus \dots \oplus \begin{matrix} V_{2i} \\ V_{2i} \end{matrix}}_{y_i \text{ times}} \oplus \underbrace{V_{2i} \oplus \dots \oplus V_{2i}}_{z_i \text{ times}} \oplus \dots$$

$$\dots \oplus \underbrace{\begin{matrix} V_i \\ V_i \end{matrix} \oplus \dots \oplus \begin{matrix} V_i \\ V_i \end{matrix}}_{y_{2i} \text{ times}} \oplus \underbrace{V_i \oplus \dots \oplus V_i}_{z_{2i}} \oplus \dots$$

Thus  $z_i = z_{2i}$  and  $x - z_i - y_i = y_{2i}$ . □

Proposition 2 implies that

$$\phi(C)^\perp = \pi(C(h)) = \pi \left( \bigoplus_{i=0}^{\nu} \underbrace{V_i \oplus \dots \oplus V_i}_{y_i + z_i \text{ times}} \right). \quad (3)$$

Since  $\ker \phi = C(h)$ , we furthermore have

$$\phi(C) \cong C / \ker \phi \cong \bigoplus_{i=0}^{\nu} \underbrace{V_i \oplus \dots \oplus V_i}_{y_i \text{ times}},$$

which leads to

$$\phi(C)^\perp / \phi(C) \cong \bigoplus_{i=0}^{\nu} \underbrace{V_i \oplus \dots \oplus V_i}_{z_i \text{ times}}.$$

Taking dimensions we get

$$\dim \phi(C)^\perp / \phi(C) = z_0 + s(p) \left( \sum_{i=1}^{\nu} z_i \right). \quad (4)$$

**Proposition 3.** *With the notations used in Proposition 2 we have*

- a)  $x \equiv w \pmod{2}$ , if  $n \equiv 0 \pmod{4}$ ,
- b)  $x \not\equiv w \pmod{2}$ , if  $n \equiv 2 \pmod{4}$ .

Furthermore, if  $s(p)$  is even, then

$$x \equiv z_1 \equiv \dots \equiv z_\nu \pmod{2}.$$

*Proof.* a) and b) follow immediately from (2). The last fact is a consequence of  $2y_i + z_i = x$ , if  $s(p)$  is even, which is stated in Proposition 2.  $\square$

**Corollary 1.**

- a)  $\phi(C)^\perp / \phi(C)$  is of even dimension, if  $n \equiv 0 \pmod{4}$ ,
- b)  $\phi(C)^\perp / \phi(C)$  is of odd dimension, if  $n \equiv 2 \pmod{4}$ .

*Proof.* First note that  $s(p) \sum_{i=1}^{\nu} z_i \equiv 0 \pmod{2}$  whatever the parity of  $s(p)$  is. In case  $s(p)$  odd this follows from  $z_i = z_{2i}$  for  $i \in \{1, \dots, 2t = \nu\}$  (see Proposition 2). Furthermore,  $z_0 \equiv x + w \pmod{2}$ , hence  $z_0$  even, if  $4 \mid n$ , and  $z_0$  odd, if  $n \equiv 2 \pmod{4}$ , according to Proposition 3. Thus (4) yields

$$\dim \phi(C)^\perp / \phi(C) \equiv z_0 \equiv 0 \pmod{2}, \text{ if } n \equiv 0 \pmod{4}$$

and

$$\dim \phi(C)^\perp / \phi(C) \equiv z_0 \equiv 1 \pmod{2}, \text{ if } n \equiv 2 \pmod{4}.$$

$\square$

**Corollary 2.** *Let  $n \equiv 0 \pmod{4}$  and let  $s(p)$  be even. If  $w$  is odd, then*

$$\dim C(h) = \dim \pi(C(h)) \geq \frac{n}{4} + \frac{s(p)\nu}{2} = \frac{n}{4} + \frac{p-1}{2}.$$

*In particular,  $\phi(C) < \phi(C)^\perp$ .*

*Proof.* By Lemma 2, the condition  $4 \mid n$  forces that  $w$  and  $x$  have the same parity. Thus  $w$  odd implies that  $x$  is odd and by Proposition 2, we get  $z_i \geq 1$  for  $i = 1, \dots, \nu$ . Therefore, according to (4),

$$\dim C(h) = \dim \pi(C(h)) \geq \frac{n}{4} + \frac{s(p)\nu}{2} = \frac{n}{4} + \frac{p-1}{2}.$$

$\square$

**Remark 5.** We may ask whether the converse of Corollary 2 holds true; i.e., does  $\phi(C) < \phi(C)^\perp$  always implies that  $w$  is odd? This is not true. For instance, there exist self-dual  $[36, 18, 8]$  codes and automorphisms of order 6 (note that  $s_2(3)$  is even) for which  $\pi(C(h))$  is not self-dual, but  $w$  is even.

**Corollary 3.** *Let  $n \equiv 0 \pmod{4}$  and let  $s(p)$  be even. If  $g$  has an odd number of cycles of order 2, then  $C$  is not projective as a  $K\langle g \rangle$ -module.*

*Proof.* If the number of 2-cycles of  $g$  is odd, then  $w$  is odd. Thus, by Corollary 2 and Theorem 1, the assertion follows.  $\square$

Let us introduce a notation about the structure of the automorphisms.

**Definition 2.** We say that an automorphism of prime order  $p$  of a code is of type  $p-(\alpha, \beta)$  if it has  $\alpha$   $p$ -cycles and  $\beta$  fixed points. Furthermore an automorphism of order  $2p$  is of type  $2p-(\alpha, \beta, \gamma; \delta)$  if it has  $\alpha$  2-cycles,  $\beta$   $p$ -cycles,  $\gamma$   $2p$ -cycles and  $\delta$  fixed points.

Since  $\text{Aut}(C) \leq \mathcal{S}_n$ , the largest possible prime which may occur as the order of an automorphism of a self-dual code of length  $n$  is  $p = n - 1$ . If  $n \equiv 0 \pmod{8}$ , then  $s(p)$  is odd. Obviously, in this case we can not have an automorphism of order  $2p$ .

Let  $C$  be an extremal self-dual code of length  $n \geq 48$ . According to Theorem 7 in [4] an automorphism of type  $p-(\alpha, \beta)$  with  $p > 5$  satisfies  $\alpha \geq \beta$ . Hence the second largest possible prime  $p$  satisfies  $n = 2p + 2$ .

**Corollary 4.** *Let  $C$  be a self-dual code of length  $n = 2p + 2$ , where  $p$  is an odd prime, and minimum distance greater than 4. Suppose that involutions in  $\text{Aut}(C)$  are fixed point free. If  $s(p)$  is even, then  $\text{Aut}(C)$  does not contain an element of order  $2p$ .*

*In case  $C$  is doubly even, the condition  $s(p)$  even may be replaced by condition  $p \not\equiv -1 \pmod{8}$ .*

*Proof.* Suppose that  $g$  is an automorphism of order  $2p$ . Thus  $g$  has a cycle of length  $2p$  and one of length 2. As above let  $h = g^p$ . By Corollary 2, we get

$$\dim \pi(C(h)) \geq \frac{n}{4} + \frac{p-1}{2} = p.$$

Since  $\pi(C(h)) \leq K^{\frac{n}{2}} = K^{p+1}$ , we see that  $\pi(C(h))$  has minimum distance 1 or 2, a contradiction.

In case that  $C$  is doubly even we only have to show that  $p \equiv 1 \pmod{8}$  does not occur (see Remark 1). If  $p \equiv 1 \pmod{8}$  then  $n = 2p + 2 \equiv 4 \pmod{8}$ , contradicting the Theorem of Gleason (see [11], Theorem Corollary 9.2.2).  $\square$

**Corollary 5.** *Let  $C$  be an extremal self-dual code of length  $n = 24m$ . Let  $g \in \text{Aut}(C)$  be an element of type  $2p-(w, 0, x; 0)$ . If  $s(p)$  is even and  $w$  is odd, then  $p \leq \frac{n}{4} - 1$ .*



*Proof.* By Corollary 2,  $\pi(C(h))$  has parameters  $[12m, \geq 6m + \frac{p-1}{2}, \geq 2m + 2]$ . According to the Griesmer bound (see [11], Theorem 2.7.4), we have

$$12m \geq \sum_{i=0}^{6m + \frac{p-1}{2} - 1} \left\lceil \frac{2m + 2}{2^i} \right\rceil \geq (2m + 2) + (m + 1) + (6m + \frac{p-1}{2}) - 2.$$

This implies  $p \leq 6m - 1 = \frac{n}{4} - 1$ .  $\square$

Clearly, the estimation in Corollary 5 is very crude for  $m$  large. For instance, if  $m = 5$  the statement in Corollary 5 leads to  $p \leq 29$ , but computing all terms in the sum shows that even  $p \leq 23$ .

## 4 Application to extremal self-dual codes of length 120

From now on  $C$  is supposed to be a self-dual  $[120, 60, 24]$  code. The following (see [7]) is the state of art about the automorphisms of  $C$ .

Automorphisms of odd prime order which may occur in  $\text{Aut}(C)$  are of type 29-(4, 4), 23-(5, 5), 19-(6, 6), 7-(17, 1), 5-(24, 0) or 3-(40, 0). Automorphisms of order 2 can only be of type 2-(48, 24) or 2-(60, 0). Automorphisms of possible composite odd order are of type 3·5-(0, 0, 8; 0), 3·19-(2, 0, 2; 0) or 5·23-(1, 0, 1; 0).

Thus we may ask about elements  $g \in \text{Aut}(C)$  of order  $2p$  where  $p$  is an odd prime. Note that the involution  $h = g^p$  has no or exactly 24 fixed points, by [5].

**Lemma 2.** *If the involution  $h$  has no fixed points, then  $g$  is of type*

- $2 \cdot 29$ -(2, 0, 2; 0),
- $2 \cdot 19$ -(3, 0, 3; 0),
- $2 \cdot 5$ -(0, 0, 12; 0),
- or  $2 \cdot 3$ -(0, 0, 20; 0).

*If  $h$  has 24 fixed points then  $g$  is of type*

- $2 \cdot 23$ -(2, 1, 2; 1),
- or  $2 \cdot 3$ -(0, 8, 16; 0).

*Note that  $\text{Aut}(C)$  does not contain elements of order  $2 \cdot 7$ .*

*Proof.* The proof is straightforward by considering the cycle-structures using [7].  $\square$

The above cycle structures show that only elements of order  $2 \cdot 19$  satisfy the hypothesis of Corollary 2. In this case  $s(19)$  is even and so we have

$$\dim C(g^{19}) \geq \frac{120}{4} + \frac{19-1}{2} = 39.$$

Thus  $\pi_2(C(g^{19}))$  is a  $[60, \geq 39, \geq 12]$  code. According to Grassl's list [8] a  $[60, \geq 39]$  code has minimum distance at most 10. Therefore we can state the following.

**Proposition 4.** *The automorphism group of an extremal self-dual  $[120, 60, 24]$  code does not contain elements of order 38.*

Next we consider automorphisms of order 58. By Lemma 2, we know that  $g$  is of type  $2 \cdot 29-(2, 0, 2; 0)$ . Therefore  $g^2$  is of type  $29-(4, 4)$  and  $g^{29}$  is of type  $2-(60, 2)$ . Thus, without loss of generality, we may assume that

$$g^2 = (1, \dots, 29)(30, \dots, 58)(59, \dots, 87)(88, \dots, 116)$$

and

$$g^{29} = (1, 30)(2, 31) \dots (59, 88)(60, 89) \dots (117, 118)(119, 120).$$

If  $\pi_{29} : C(g^2) \rightarrow \mathbb{F}_2^8$  is defined by

$$(v_1, \dots, v_{120}) \mapsto (v_1, v_{30}, v_{59}, v_{88}, v_{117}, v_{118}, v_{119}, v_{120})$$

then  $\pi_{29}(C(g^2))$  is a self-dual  $[8, 4]$  code according to [10]. and clearly, the minimum distance must be greater or equal to 4 since  $C$  is doubly-even. It is well-known that, up to equivalence, the only code with such parameters is the extended Hamming code  $\hat{\mathcal{H}}_3$ .

According to Lemma 1 the structure of the ambient space  $K^{120}$ , viewed as a module for the group  $\langle g \rangle$ , is as follows:

$$K^{120} = \begin{matrix} K & K & K & K \\ K & K & K & K \end{matrix} \oplus \begin{matrix} V & V \\ V & V \end{matrix}$$

where  $\dim V = 28$ . Since  $C(g^2)$  has dimension 4, the code  $C(g) = (C(g^2))(g^{29})$  has dimension at least 2. By calculations we verify that

$$\dim((\pi_{29}^{-1}(A))(g)) \leq 2$$

for every  $A \in \hat{\mathcal{H}}_3^{S_8}$ , which denotes the set of all self-dual  $[8, 4, 4]$  codes. Note that there are only a few computations since  $|\hat{\mathcal{H}}_3^{S_8}| = \frac{|S_8|}{|\text{Aut}(\mathcal{H}_3)|} = 30$ . Thus  $\dim C(g) = 2$  and there are only two possible structures for  $C$ , namely

$$\text{a) } C = \begin{matrix} K & K \\ K & K \end{matrix} \oplus V \oplus V \quad \text{or}$$

$$\text{b)} \quad C = \begin{matrix} K & K \\ K & K \end{matrix} \oplus \begin{matrix} V \\ V \end{matrix}.$$

Next we look at  $C(g^{29})$  which may be written as  $C(g^{29}) = B \otimes \langle (1, 1) \rangle$ , where  $B = \pi_2(C(g^{29}))$  is a  $[60, \geq 30, \geq 12]$  code. In case a) we have  $\dim B = 58$ , a contradiction. Thus case b) occurs. According to Theorem 1,  $C$  is projective and  $B$  is a self-dual  $[60, 30, 12]$  code. Furthermore  $B$  has an automorphism of type 29-(2, 2).

**Proposition 5.** *Every self-dual  $[60, 30, 12]$  code  $B$  with an automorphism of type 29-(2, 2) is bordered double-circulant. There are (up to equivalence) three such codes.*

*Proof.* We can easily determine the submodule of  $B$  fixed by the given automorphism and then do an exhaustive search with MAGMA on its complement in  $K^{60}$  (following the methods described in [10] and considering the complement as a vector space over  $\mathbb{F}_{2^{28}}$ ). In fact, it turns out that  $B$  is equivalent to one of the three bordered double-circulant singly-even codes of length 60 classified by Harada, Gulliver and Kaneta in [9].  $\square$

It is computationally easy to check that there are exactly 14 conjugacy classes of elements of type 29-(2, 2) in  $\text{Aut}(B)$  for each of the three possibilities for  $B$ .

Using this we are able to do an exhaustive search for  $C$  along the methods used in [2]. Without repeating all the details, we just recall the two main steps of the search. First we determine a set, say  $\mathcal{L}$ , such that there exists a  $t \in \mathcal{S}_{120}$  and  $L \in \mathcal{L}$  such that  $(C(g^2) + C(g^{29}))^t = L$  and  $g^t = g$ . It turns out that  $|\mathcal{L}| = 42$ . In the second step we construct all possible codes  $C$  from the knowledge of its socle as in section VI of [2]. By checking the minimum distance we see that in all cases the codes are not extremal which proves the following.

**Proposition 6.** *The automorphism group of an extremal self-dual  $[120, 60, 24]$  code does not contain elements of order 58.*

**Acknowledgment.** The first author likes to express his gratitude to his supervisors F. Dalla Volta and M. Sala. Both authors are indebted to the *Dipartimento di Matematica e Applicazioni* at Milano and the *Institut für Algebra und Geometrie* at Magdeburg for hospitality and excellent working conditions, while this paper has mainly been written. *Laboratorio di Matematica Industriale e Crittografia* of Trento deserves thanks for the help in the computational part.

## References

- [1] E. F. Assmuss, H.F. Mattson, *New 5-designs*, J. Combin. Theory 6 (1969) 122–151.

- [2] M. Borello, *The automorphism group of a self-dual  $[72, 36, 16]$  binary code does not contain elements of order 6*, to appear IEEE Trans. Inform. Theory.
- [3] S. Bouyuklieva, *A method for constructing self-dual codes with an automorphism of order 2*, IEEE Trans. Inform. Theory 46, No. 2 (2000), 496–504.
- [4] S. Bouyuklieva, A. Malevich and W. Willems, *Automorphisms of extremal codes*, IEEE Trans. Inform. Theory 56 (2010), 2091–2096.
- [5] S. Bouyuklieva, *On the automorphisms of order 2 with fixed points for the extremal self-dual codes of length  $24m$* , Des. Codes Cryptogr. 25 (2002) 5–13.
- [6] W. Bosma, J. Cannon, C. Playoust, *The MAGMA algebra system I: The user language*, J. Symbol. Comput. 24 (1997) 235–265.
- [7] J. de la Cruz, *Über die Automorphismengruppe extremaler Codes der Längen 96 und 120*, PhD thesis, Otto-von-Guericke University Magdeburg.
- [8] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, online available at [www.codetables.de](http://www.codetables.de), accessed on 2012-09-15
- [9] M. Harada, T.A. Gulliver and H. Kaneta, *Classification of extremal double-circulant self-dual codes of length up to 62*, Discrete Mathematics 188 (1998), 127–136.
- [10] W.C. Huffman, *Automorphisms of codes with application to extremal doubly even codes of length 48*, IEEE Trans. Inform. Theory 28 (1982), 511–521.
- [11] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003.
- [12] B. Huppert and N. Blackburn, *Finite Groups II*, Springer 1982.
- [13] C. Martínez-Pérez and W. Willems, *Self-dual codes and modules of finite groups in characteristic two*, IEEE Trans. Inform. Theory 50 (2004), 67–78.
- [14] E.M. Rains, *Shadow bounds for self-dual codes*, IEEE Trans. Inform. Theory 44 (1998), 134–139.
- [15] W. Willems, *A note on self-dual group codes*, IEEE Trans. Inform. Theory 48 (2002), 3107–3109.